基于 BP 网络判断传感器数据可信度研究 *

刘小久，袁　丁†，梁瑷云，严　清

(四川师范大学 计算机科学学院, 成都 610101)

摘　要：传统方法使用对称及非对称加密对传感器网络系统进行安全保障，需要大量的加解密计算且在密钥被破解后不能准确判断数据的可信性，不能有效保证无线传感器网络系统安全。为保障无线传感器网络系统安全，针对无线传感器网络中节点信息可信度问题，提出了一种基于 BP 网络判断节点信息可信度的方法。该方法在边界路由器上使用 BP 神经网络，对采集的多特征值数据进行训练，然后用训练所得结果判断节点可信度，进而筛选出数据。该方法具有较低的系统开销与较高的安全保证，能够筛选出问题节点，并保证传感器网络的安全运行。实验结果表明，该方法认证时间短，能达到预期效果。

关键词：BP 网络；无线传感器网络；传感器节点；可信性；安全性

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.02.0171

Research on data credibility of sensor based on BP network

Liu Xiaojiu, Yuan Ding†, Liang Aiyun, Yan Qing

(*School of Computer Science Sichuan Normal University*, *Chengdu* 610101, *China*)

Abstract: The traditional method uses symmetric encryption and asymmetric encryption to secure the sensor network system, which requires a lot of encryption and decryption calculations and the credibility of the data cannot be accurately judged after the key cracked. The encryption method hardly guarantee the safety of wireless sensor network system effectively. This paper proposed a method determining the reliability of node information based on BP network to ensure the security of wireless sensor network system by the credibility of node information in wireless sensor networks. The method used BP neural network on the border router to train the collected data of multiple eigenvalues and determine the credibility of the node with training results to filter the data. The BP network judgment method could achieve lower system overhead and higher security assurance without additional communication data or calculation tasks. What's more, this method could screen problem nodes to ensure the safe operation of the sensor network. Experiment confirm that this method with a short authentication time cost and can achieve the desired results.

Key words: BP network; wireless sensor networks; sensor nodes; creditability; security

0　引言

无线传感器网络(wireless sensor networks,WSN)是目前物联网技术研究的热点，其不需要基础设施支持，而且可以迅速在指定区域内布置传感器节点，用于环境状况检测，同时通过无线链路向基站报告，是一种非常灵活的无线网络结构。WSN 适用于敌对环境或大规模地理区域，在军事及民用领域得到广泛应用，如目标跟踪、区域侦查及野外环境监测。一些特殊应用场景包括：a)军事领域，WSN 可以应用于军事方面，例如战场上，传感器节点可以监视敌军汽车流量或监测敌军行动位置；b)环境监测，例如监控森林火灾情况，或者随机散落在易污染环境中，监控环境受污染情况的原始数据。

WSN 节点可采用飞机抛撒或随机散落等方式进行布置，一般不受人为因素影响。但在自然环境中，磁场干扰、电场干扰、非法攻击等因素会导致无线传感器节点传送非法数据。为保证 WSN 系统安全运行，节点信息安全随之被提出。传统节点安全通信方案是使用对称加密方法对节点传输的信息进行加密，使用非对称加密方法对节点身份进行认证。该方案需要极大的运算量。由于传感器节点运算能力有限，不便于进行大量的加、解密运算，且在密钥被破解后安全问题不能得到很好的保障。

收稿日期：2018-02-07；**修回日期：**2018-04-16　**基金项目：**国家科技支撑计划资助项目（2014BAH11F01）；国家自然科学基金资助项目（61373163）；四川省可视化与虚拟现实软件重点实验室项目

作者简介：刘小久（1989-），男，湖北随州人，硕士研究生，主要研究方向为数据挖掘、信息安全（2022466130@qq.com）；袁丁（1967-），男（通信作者），四川宜宾人，教授，博士，主要研究方向为数据挖掘、信息安全；梁瑷云（1992-），女，四川广元人，硕士研究生，主要研究方向为数据挖掘、信息安全；严清（1985-），男，四川南充人，硕士，讲师，主要研究方向为信息安全.

为降低节点运算量，延长无线传感器网络的生命周期，并提高系统安全性能，本文提出了一种基于 BP 网络判断节点数据可信度的方法，以清除干扰数据，同时提高系统可运行性。

1 相关工作

随着传感器网络技术的大规模应用，节点的安全问题提出后，传统保证无线传感器网络数据安全采用的方法主要有三种：

a)数据加密及身份认证。文献[1~7]提出采用加密的方式对无线传感器节点间传输的数据进行保护。该方法使用非对称加密算法对传感器网络中节点的身份进行认证，使用对称加密算法对传感器节点间传送的信息进行加密传输。数据加密及身份认证在一定程度上可以保证节点传送信息的安全，但忽略了节点计算能力和能量有限的情况。因为无线传感器网络中的节点是一个计算能力和能量有限的单位，传统的数字签名安全认证方法要求高计算能力和高能量，所以传统的数字签名方法[8]已经不再适用于无线传感器网络中的安全节点认证。

b)路径规划。对无线传感器网络节点间传输数据的路径进行规划，让节点信息在安全的路径中传输，文献[9~10]基于此方法进行了相应的探索。该方法在节点布置完毕后对传输信息的路径进行规划。由于无线传感器网络是一种自组织网络，节点的稳定性存在不确定因素，任意路径中的节点缺失都可能导致网络中大部分节点不可用，影响网络的可用性。路径规划限制了无线传感器网络的运行，不能保证网络的稳定。

c)私有协议传输。文献[11~17]提出为保证传输的可靠性，对无线传感器网络节点间的通信使用私有通信协议。使用私有协议进行通信在一定程度上可以保证节点间通信的安全性。但随着物联网技术的发展，封闭的协议不利于系统的扩展及大规模应用。

上述三种方法在一定程度上能够保证节点信息传输的安全性。但对已俘获的节点，非法入侵者伪造非法数据干扰系统，或者由于传感器节点自身原因及环境因素影响而发送错误数据，导致上述方法不能很好地进行安全防范。

近年来机器学习等方法也应用到信息安全中[18]，但在传统网络中使用机器学习进行安全防范有其自身的局限。首先，攻击者可以根据机器学习中相应的安全策略恶意构建输入以迫使错误分类[19]，来达到合法攻击的目的；其次，机器学习方法建立在对攻击者构建的防御机制有限的基础上，攻击往往会对敌人的知识和能力作出不切实际的假设[20]。然而无线传感器网络中由于节点功能的单一以及安全防范的明确性，机器学习方法可以很好地应用到无线传感器网络中。

为验证节点发送数据的可信任性，苗成林[21]提出基于 D-S 证据理论的传感器可信性度量算法。该算法在检测到系统异常后，会验证数据的可信性，然后作出相应的操作。但是这种方案设计具有被动性，系统在监测到异常后才会对数据进行可信性判断。

基于上述研究，本文提出了一种基于 BP 神经网络的无线传感器节点数据可信性识别的方法，对节点发送的信息进行判断，得到节点发送信息的可信性。

2 基于 BP 神经网络解决方案设计

根据无线传感器节点的特性，基于 BP 神经网络学习算法，使用 BP 神经网络对传感器节点进行可信度判断。

2.1 BP 神经网络结构

BP 神经网络由输入层、隐藏层和输出层构成。输入层将训练样本送入网络，隐藏层对样本数据进行训练。理论证明，在隐藏层节点数目合理的情况下 BP 神经网络仅需要三层就具有模拟任意复杂非线性映射的能力[22]。本文采用三层结构的BP 神经网络。BP 神经网络结构如图 1 所示。

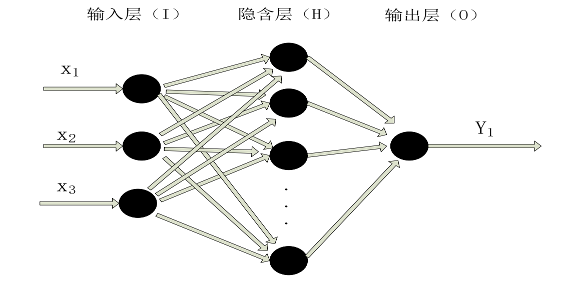


图 1　BP 神经网络结构示意图

输入层节点和输出层节点数目是确定的，隐藏层节点数一般采用试算法来确定，其最佳神经元数量经验公式为

$$h = \sqrt{m+n} + a \tag{1}$$

其中：h 为隐藏层节点数目；m 为输入层节点数目；n 为输出层节点数目；a 为[1,10]间的调节常数。

2.1.1 正向传递子过程

设节点 i 与 j 之间的权值为W_{ij}，节点 j 的阈值为b_j，节点的输出值为x_j。节点输出值根据上层所有节点输出值、节点权值、阈值及激活函数等一系列变换后得到。具体计算方法如下：

$$S_j = \sum_{i=0}^{m-1} w_{ij}\, x_i + b_j \tag{2}$$

$$x_j = f(S_j) \tag{3}$$

其中：f 为激活函数，一般选取 Sigmoid 型函数，如式（4）所示。

$$f(\theta) = \frac{A}{1+e^{-\frac{\theta}{B}}} \tag{4}$$

其中：A、B 为常数。这样 BP 网络就完成了由 n 维空间向量向 m 维空间向量的近似映射。

2.1.2 反向传递子过程

BP 神经网络的主要目的是反复修正权值和阈值，使得误差值达到最小。在 BP 神经网络中，假设输出层中第 j 个节点的实际结果为d_j，期望结果为y_j，则误差E的计算公式如式(5)所示。

$$E(\omega,b) = \frac{1}{2}\sum_{j=0}^{n-1}(d_j - y_j)^2 \tag{5}$$

隐藏层(输入层)与输出层(隐藏层)之间的权值和阈值调整

如下：

$$\omega_{ij} = \omega_{ij} - \eta_1 \times \frac{\partial E(\omega, b)}{\partial \omega_{ij}} = \omega_{ij} - \eta_1 \delta_{ij} x_i \qquad (6)$$

$$b_j = b_j - \eta_2 \times \frac{\partial E(\omega, b)}{\partial b_j} = b_j - \eta_2 \delta_{ij} \qquad (7)$$

其中：ω_{ij}为待修正的权值；b_j 为待修正的阈值；η_1，η_2 为预先规定的学习速率；δ_{ij}为隐藏层(输入层)节点 i 到输出层(隐藏层)节点 j 的动量因子。

2.1.3 应用原理介绍

由于稳定的无线传感器网络节点发送的都是具有一定规律的环境数据，与 Internet 中人类发送的交互数据相比，具有单一性。对这种单一条件下的数据可以对其进行相应的分类。

BP 神经网络是一种按照误差逆向传播算法训练的多层前馈神经网络，是分类算法中的一种。其对现有的已分类数据进行训练后，可以使用训练结果对未知的数据通过其特征值判断其属性。与其他分类算法相比，BP 网络结构简单，操作方便，在性能和准确度方面，适合于对无线传感器节点的可信性进行判断。

2.2 安全方案设计

无线传感器节点一般布置在公共场合，收集周围的环境信息。系统运行中，非法攻击者可以通过监听等手段获取无线传感器网络的通信数据，经过脱密处理后，攻击者可以伪装成合法节点发送信息对系统进行干扰，导致系统错报或者误报，达到扰乱系统的目的。传统的安全保障方法对这种攻击方法不能很好地防范。此外环境因素，如磁场干扰、电场干扰等会导致传感器节点随机发送不稳定数据，也可造成系统误报。

为防止攻击者伪造信息及环境影响发送错误信息，本方案提出使用 BP 神经网络的方法对节点收集的信息进行判断，滤除虚假信息及干扰数据。

2.2.1 数据流程及系统运行流程

传感器节点收集的数据经区域内路由后，到达边界路由器。在边界路由器中，设置 BP 神经网络判断方法对节点数据的可信性进行判断。如果节点信息可信，则传输给服务器；如果节点信息不可信，则丢弃。在无线传感器网络中，节点发送的信息包括正常数据、环境影响下发送的错误数据、攻击者发送的伪造数据。数据流程如图 2 所示。

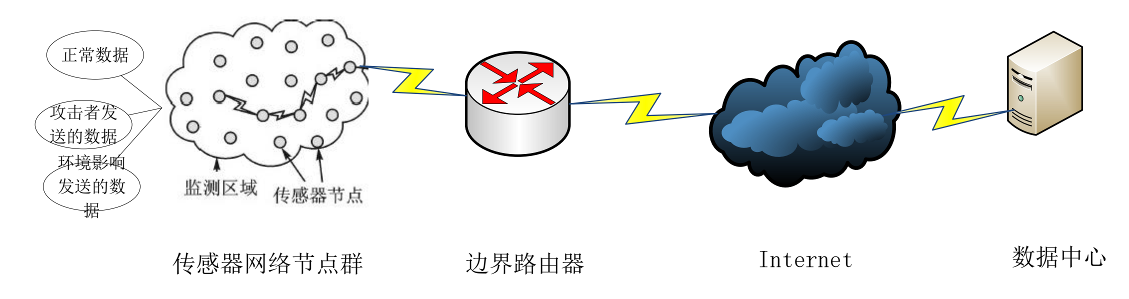


图 2　无线传感器数据流程

系统运行分为数据收集、数据训练、正常运行三个阶段。

第一阶段：数据收集阶段。边界路由器收集两轮节点发送的数据，收集完 N 个节点信息为一轮。在该阶段，仅对数据进行收集转发，不对数据进行相应的判断，并且设定节点初始信任值。相当于边界路由器对前两轮收集到的数据完全信任。

第二阶段：数据训练阶段，在第三轮数据收集开始时，训练启动。当训练过程启动时，边界路由器继续收集、转发数据，并且预设数据初始信任值。在该阶段不对数据进行判断。需要在第三轮收集数据期间启动训练过程，是因为时间频率作为训练数据集的一个特征值，需要获取相应的时间频率。在此阶段，边界路由器依旧信任收集到的数据。

第三阶段：正常运行阶段。当第三轮数据收集完毕后，系统进入正常运行阶段。在该阶段，当边界路由器收到数据时，需要使用训练结果集对收到的数据进行判断，然后根据判断的结果作出相应的操作。在判断期间，系统会继续训练上轮收集的数据。系统能够在该阶段对收到的数据进行判断，是因为经过第三轮的数据收集，训练过程已经完毕，结果集已经获得。系统总流程如图 3 所示。

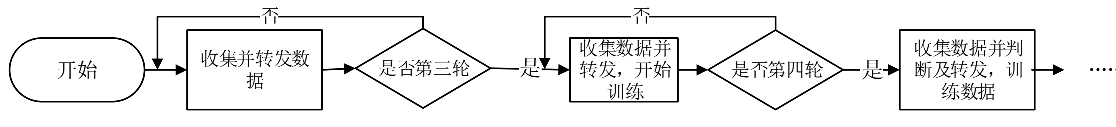


图 3　系统运行流程

2.2.2 判断过程

传感器节点传输的是一些简单的信息，如温度、光照、湿度、地面震动频率、红外感应强度、环境噪声、电池电量释放曲线等环境信息。本文抽取节点传送的具有一定意义的特征信息，使用 BP 神经网络进行训练，得出训练后的结果集。当节点再次发送信息时，使用训练得到的相关参数对节点发送的信息进行判断。如果判断后的结果在绝对可信的范围内，则进行转发，并把该信息加入训练集；如果判断后的结果在相对可信的范围内，则该信息可以作为训练值参加后续的训练过程，但节点信息不转发；如果判断后的值绝对不可信，则直接丢弃。这样动态的认证节点发送的信息，不需要对节点传输的身份信息进行加密，不用考虑非法节点的伪造，节省了节点的运算时

间，延长了节点的使用寿命。判断结果及操作如表 1 所示，判断流程如图 4 所示。

表 1　判断结果及操作

判断后结果	操作	结果
绝对可信	加入训练集	转发
相对可信	加入训练集	不转发
绝对不可信	不加入训练集	不转发

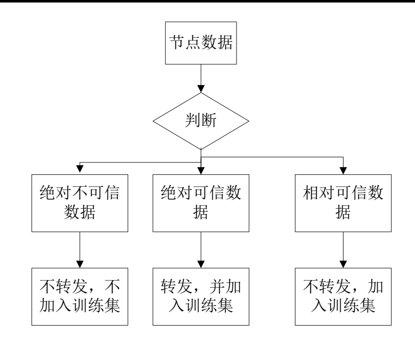


图 4　判断流程

2.2.3 学习过程

抽取的特征信息包括节点发送的温度、光照、湿度、节点发送数据的频率、地面震动频率、红外感应强度、环境噪声、电池电量释放曲线。正常温度、湿度、光照、红外感应强度、地面震动频率等，环境数据的升高和降低都是一个缓慢渐变的过程，不可能陡然提高或者陡然降低，而环境噪声、电池电量释放曲线等环境信息相对稳定。在火灾、水灾等情况下，环境数据升高或降低也是一整片节点升高或者降低，不可能某一个节点数据突然升高或者突然降低。如果某个节点数据突然跃迁，可以判断为非法信息。若整片节点跃迁，准确信息第一次可能不会发送到服务器，第二次则可以发送到服务器，时间相隔不会超过节点发送信息的频率。由于系统稳定后，节点发送数据频率稳定，周围环境也趋于稳定，电池电量释放情况同样趋于稳定，所以采用这八个维度的数据作为特征数据。

选取的节点特征信息及判定信息如表 2 所示。

表 2　特征信息及判定信息

特征信息(输入)	判定信息(输出)
节点基础信息传输频率	
环境光照	
温度湿度	
地面震动频率	
红外感应强度	可信度(%)
环境噪声	
电量释放曲线	
节点认证兄弟节点规模	

在前三次信息收集中，可信度自行设置。第三次收集信息时，BP 神经网络对收集到的数据进行训练，该次收集完毕，训练结果集即可获得，以后收集到的信息就可以使用 BP 神经网络训练的结果集进行判断。在判断过程中，本次判断所使用的结果集是根据前一次训练后的数据得来的。

判断时使用的计算公式如式(2)~(4)所示。

2.2.4 训练方法

由于不需要对节点数据进行删除、修改等操作，所以可在边界路由器中使用数组结构保存节点数据。数组结构如下：

```
float  M[10000][9];
```

使用二维数组保存节点信息，第一维用于保存节点编号，第二维用于保存节点发送信息的频率、温度、光照、湿度、地面震动频率、红外感应强度、环境噪声、电池电量释放曲线、时间戳。时间戳为收到节点数据时的时间戳，频率数据为该次的时间戳减去上次收到节点数据的时间戳。第一轮收集数据时，时间频率为时间戳。

节点发送信息的频率、温度、光照、湿度、地面震动频率、红外感应强度、环境噪声、电池电量释放曲线作为在 BP 神经网络中输入层的输入数据。当第三次收集信息时，BP 神经网络训练过程开始。以后每一轮收集完毕，BP 网络开始训练。

3　实验设计与结果对比分析

本文使用的方法是基于 BP 神经网络的安全认证方法，不需要对节点的信息进行非对称密钥加密，不需要过多地关注节点本身的情况即可判断信息的可信与不可信情况。

3.1　实验环境

本实验使用具有 2 GB 内存，Core 单核处理器，安装有 Ubuntu 14.04 系统的计算机作为边界路由器。在边界路由器中配置运行环境，并且安装 Workerman 框架。实验将台式计算机作为边界路由器，其目的在于在边界路由器上搭建 BP 神经网络，实现输入数据的可信度验证。

本实验通过分析真实环境下传感器节点使用公共协议 lOWPAN_IPHC 发送的数据，采用编程的方式自动生成模拟数据(其中包含小部分的干扰数据)作为本文实验的数据来源。本实验只对节点的安全认证进行验证，不考虑客户机端的数据情况。

3.2　实验方法

假设无线传感器区域拥有 N 个节点，每个节点每 M 时间间隔发送一次收集到的环境信息。

无线传感器节点持续收集周围环境信息，并且发送给边界路由器。边界路由器会记录收到数据时的时间，时间频率作为 BP 神经网络的一个有效输入特征。另几个特征为节点传输的温度、光照、湿度、地面震动频率、红外感应强度、环境噪声、电池电量释放曲线。

系统运行在数据收集、数据训练、正常运行三个阶段的具体过程如下：

a)数据收集阶段。

该阶段，边界路由器收集两轮节点发送的数据。在收集第一轮数据时，所有节点数据存储于数组中；当第二轮数据收

集时，用收集到的节点时间戳减去第一轮相同数据节点的时间戳，以获取节点发送数据时间间隔。期间，边界路由器仅对数据进行转发，不对数据进行相应的判断，并且设定初始的信任值。在实验中，设定的初始值为 9.859~9.889 间的随机数。该数据区域是根据需要自主设定，区间可以任取。当两轮数据收集完毕后，收集数据阶段完毕。

b)数据训练阶段。

第三轮收集数据时，训练过程启动。需要在第三轮收集数据期间启动训练过程，是因为时间频率作为训练数据集的一个特征数据，需要有时间频率相应值。当收集两轮数据后，时间频率值即可获得。训练过程启动时，边界路由器继续收集、转发数据，但不对数据进行判断，并且预设数据初始信任值。

c)正常运行阶段。

当第三轮数据收集完毕后，系统进入正常运行阶段，即当边界路由器收到数据时，使用训练结果集对收到的数据进行判断，然后根据判断的结果做出相应的操作，同时边界路由器训练上轮收到的数据。边界路由器在该阶段能够对收到的数据进行判断，是因为经过第三轮的数据收集，训练过程已经完成，结果集已经获得。经过第三轮的数据收集，系统在后续数据收集及数据判断过程中，会对上次的收集结果进行训练。

判断后转发规则如下：如果判断后的值在初始设定的值即 9.859~9.889 间，则数据为绝对可信数据，将收到的数据加入训练池中，并且转发数据；如果判断后的值在 9.0~9.859 间或者在 9.859~10.4 间，则数据为相对可信数据，将数据加入训练池中，不转发数据；如果判断后的值在其他范围内，数据不转发，也不加入训练池中，训练后的数据用 9.859~9.889 间的任意值代替。区间及判定结果如表 3 所示。

表 3　数据区间及判定结果

区间	≤9.0	9.0≤r≤9.859	9.859≤r≤9.889	9.889≤r≤10.4	≥10.4
判定结果	绝对不可信	相对可信	绝对可信	相对可信	绝对不可信

绝对可信的区间取值根据需要自主设定。可以取值为百分位精度，也可以为千分位精度。相对可信区间取值、绝对不可信区间取值也是根据数据量需要自主设定。由于本实验是进行验证实验，对取值按照预设自主设定。

3.3　实验结果分析

在上述实验设计和实验环境下，对基于 BP 神经网络的无线传感器节点数据可信性进行验证。

对 N 个节点的数据，经过 1 000 次测试。选取 1 000 次测试作为标准，是因为 1 000 次测试的效果能够代表传感器网络正常运行的情况，增加测试次数对实验效果几乎没有提升。前三次训练时，假设节点发送的数据都是合法的数据，对以后的数据，每轮发送 N/30 个数据作为干扰数据。实验情况与结果如表 3 所示。在节点数目分别为 1 000、2 000、3 000、5 000、10 000 个的情况，设置相应的干扰数据，分别为 33、66、99、165、333 个，分别进行 100 次训练后的操作，测试后的结果如表 4 所示。

正确率计算方法为

$$\text{正确率} = \frac{\text{平均接受数据}}{\text{发送数据}-\text{干扰数据}} \times 100\% \quad (8)$$

表 4　实验结果

节点发送数据	干扰数据	平均接收数据	平均过滤数据	正确率/%
1000	33	901.55	98.45	93.2
2000	66	1798.72	201.28	93.0
3000	99	2631.96	368.04	90.8
5000	165	4633.12	366.88	95.8
10000	333	8995.32	1004.68	93.1

当节点数目增加，干扰数据增加正确率变化规律如图 5 所示。

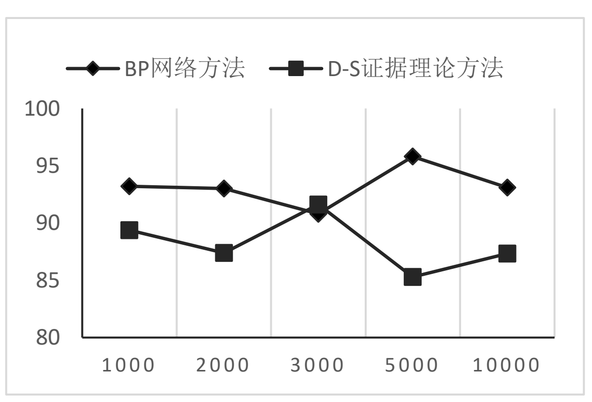


图 5　正确率变化图

从图 5 可知，随着节点数目的变化，BP 神经网络判断节点可信度的准确率在 93%上下波动，不过仍然达到 90%以上。分析原因，可能与节点传输数据时系统稳定性有关，随着节点大量连续传输数据，系统运行稳定性存在不确定因素。

本实验准确率与文献[21]提出的 D-S 证据理论方法进行对比，准确率显著提高。分析原因，文献[21]中使用的方法对节点传输数据的关联函数采用固定关联参数，由于环境变化是随机的，采用固定的参数不能代表所有的环境情况。

4　结束语

本文所提出的方法能够准确地判断非法数据的干扰，并且清除干扰数据。与文献[21]提出的 D-S 证据理论方法进行对比，准确率显著提高。在本实验中仍有改进的地方：a)改进数据的收集方法，本方法使用的是对数据传输一轮后进行训练，可以改进为经过多少时间后进行训练，便于一些其他情况的应用；b)改进数据的训练方法，本实验对数据的训练是规定的训练次数及训练参数，可以设置变动的参数对数据进行训练；c)改进

数据的存储方法，本实验使用的是数组对传输的数据进行训练，可以使用文件存储的方法对数据进行存储，减少内存开销；d) 与传统的安全保障方法相结合，进一步提升系统安全性。

参考文献：

[1] Yuan Jianjun. An enhanced two-factor user authentication in wireless sensor networks [J]. Telecommunication Systems, 2014, 55 (1): 105-113.

[2] He Daojing, Chen Chun, Chan S, *et al.* Analysis and improvement of a secure and efficient handover authentication for wireless networks [J]. IEEE Communications Letters, 2012, 16 (8): 1270-1273.

[3] Wang Ding, He Debiao, Wang Ping, *et al.* Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Trans on Dependable & Secure Computing, 2015, 12 (4): 428-442.

[4] Wang Chenyu, Xu Guoai, Sun Jing. An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks [J]. Sensors, 2017, 17 (12): 2946-2965.

[5] Li Xiong, Niu Jianwei, Kumari S, *et al.* A three-factor anonymous authentication scheme for wireless sensor networks in Internet of things environments [J]. Journal of Network & Computer Applications, 2018, 103 (2): 194-204.

[6] Wang Ding, Wang Ping. Two birds with one stone: two-factor authentication with security beyond conventional bound [J]. IEEE Trans on Dependable & Secure Computing, 2016, PP (99): 1.

[7] 陈蕾，魏福山，马传贵. 一种可证安全的面向无线传感器网络的双因素用户认证密钥协商方案 [J]. 计算机应用研究, 2016, 33 (5): 1514-1521. (Chen Lei, Wei Fushan, Ma Chuangui. provably-secure two-factor user authentication key exchange scheme for wireless sensor networks [J]. Application Research of Computers, 2016, 33 (5): 1514-1521.)

[8] 范红. 数字签名技术及其在网络通信安全中的应用 [J]. 中国科学院大学学报, 2001, 18 (2): 101-104. (Fan Hong. Applications of digital signature in network communication security [J]. Journal of Graduate School of Chinese Academy of Social Sciences, 2001, 18 (2): 101-104.)

[9] 孙亚慧，李峰. 一种基于路径的双向认证机制 [J]. 电子科技, 2017, 30 (2): 177-179. (Sun Yahui, Li Feng A mutual authentication mechanism based on the path [J]. Electronic Science and Technology, 2017, 30 (2): 177-179.)

[10] 陈建钧. 无线传感器网络中基于信任链的信任模型研究 [D]. 成都：成都信息工程学院, 2015. (Chen Jianjun. Study on trust model for wireless sensor networks based on trust chain [D]. Chengdu: Chengdu University of Information Technology, 2015.)

[11] 曹征. 无线传感器网络节点认证协议研究 [D]. 成都：西南交通大学, 2015. (Cao Zheng. The research of nodes authentication protocol for wireless sensor networks [D]. Chengdu: Southwest Jiaotong University, 2015)

[12] 郭萍，傅德胜，成亚萍，等. 一种无线传感器网络双向认证协议设计及证明 [J]. 计算机科学, 2015, 42 (2): 100-102. (Guo Ping, Fu Desheng, Cheng Yaping, *et al.* Design and proof of bilateral authentication protocol for wireless sensor network [J]. Computer Science, 2015, 42 (2): 100-103.)

[13] 孙二坤. 无疑传感器网络中安全路由协议的研究 [D]. 西安：西安电子科技大学, 2013. (Sun Erkun. The study on the security routing in the wireless sensor network [D]. Xi’an: Xidian University, 2013.)

[14] 韩笑娜. 基于信任评估的无线传感器网络安全分簇协议研究 [D]. 北京：北京航天航空大学, 2015. (Han Xiaona. Research on secure clustering protocol based on trust evaluation for wireless sensor networks [D]. Beijing: Beihang University, 2015.)

[15] 杨旻. 基于分簇的无线传感器网络安全协议研究 [D]. 桂林：桂林电子科技大学, 2014. (Yang Min. Research on cluster-based secure protocol for wireless sensor network [D]. Guilin: Guilin University Of Electronic Technology, 2014.)

[16] 黄彬，刘广钟，徐明. 基于簇的无线传感器网络安全节点认证协议 [J]. 计算机工程, 2016, 42 (7): 117-122. (Huang Bin, Liu Guangzhong, Xu Ming. Security authentication protocol for nodes in wireless sensor networks based on clusters [J]. Computer Engineering, 2016, 42 (7): 117-122.)

[17] 仇各各，汪学明，张言胜. 基于 HECC 的 WSN 身份认证协议研究 [J]. 信息网络安全, 2015, 26 (12): 54-58. (Qiu Gege, Wang Xueming, Zhang Yansheng. Research on WSN identity authentication protocol based on HECC [J]. Netinfo Security, 2015, 26 (12): 54-58.)

[18] Huang Ling, Joseph A D, Tygar J D, *et al.* Adversarial machine learning [C]// Proc of ACM Workshop on Security and Artificial Intelligence. 2011: 43-58.

[19] Huang S, Papernot N, Goodfellow I, *et al.* Adversarial attacks on neural network policies [C]// Proc of the 5th International Conference on Learning Representations. 2017: 1-7.

[20] Suciu O, Mărginean R, Kaya Y, *et al.* When does machine learning FAIL?Generalized transferability for evasion and poisoning attacks [J]. arXiv: 1803. 06975v1, 2018.

[21] 苗成林. 无线传感器网络中的可信性问题研究 [D]. 合肥：中国科学技术大学, 2014. (Miao Chenglin. Research on trustworthiness problems in wireless sensor networks [D]. Hefei: University of Science and Technology of China, 2014.)

[22] Bartkowiak A. Neural networks and pattern recognition [M]// Academic. 1998.